第1卷 第1期 铁道科学与工程学报 Vol.1 No.1
2004年7月 JOURNAL OF RAILWAY SCIENCE AND ENGINEERING July 2004

安全椭圆曲线的选择

文铁华[1],汪朝晖[2],胡湘陵[1]

(1.中南大学 信息科学与工程学院,湖南 长沙 410075;2.武汉大学 数学统计学院,湖北 武汉 430076)

摘 要:通过分析椭圆曲线离散对数问题(ECDLP)目前已知的多种攻击算法,讨论了几种特殊椭圆曲线的安全性隐患,并提出了一套完整的椭圆曲线安全准则。

关键词:椭圆曲线密码;椭圆曲线离散对数问题;安全准则

中图分类号:TN918 **文献标识码**:A **文章编号**:1672-7029(2004)01-0090-04

Selection of secure elliptic curves

WEN Tie-hua[1], WANG Zhao-hui[2], HU Xiang-ling[1]

(1. College of Information Science & Engineering, Central South University, Changsha 410075, China;
2. School of Math. & Stat., Wuhan University, Wuhan 430076, China)

Abstract: The multiple algorithms solving elliptic curve discrete logarithm problems (ECDLP) is analysed, the insecurities of several special elliptic curves over sinite fields are discussed, and a set of principles of the security of elliptic curves over finite fields is proposed.

Key words: elliptic curve cryptosystem; elliptic curve discrete logarithm problems; principles of the security

自1985年Neal Koblitz[1]和Victor Miller[2]提出椭圆曲线密码(ECC)以来,密码学和数学工作者就ECC安全性的基础问题——椭圆曲线离散对数问题(ECDLP)作了大量的研究,提出了许多求解ECDLP的算法,解决了ECC应用中的诸多安全问题。

定义1 有限域上的椭圆曲线 设E_q(q为素数或素数的幂)为有限域,$|F_q| = q$,有下述投影Weierstrass方程:

$$E: y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \quad (1)$$

a_1、a_2、a_3、a_4、$a_6 \in E_q$,则F_q上的椭圆曲线(记为$E(F_q)$)是投影平面$p^2(F_q)$上满足方程(1)的点的集合。

定义2 椭圆曲线离散对数问题(ECDLP) 设$|E(F_q)| = N$(N为大整数),P为$E(F_q)$的生产元点,即通过$E(F_q)$上的加法规则可使$E(F_q) = (P)$,则椭圆曲线离散对数(ECDLP)问题为:已知P和另一点$Q \in E(F_q)$,求a($a \in \{0,1,\cdots,N-1\}$),使得$Q = aP$。

椭圆曲线的安全性是指为实现ECC而选取的椭圆曲线上EDLP的难解性,即求解该ECDLP的最有效算法的时间复杂度,安全的椭圆曲线上的ECDLP是不能被所有的已知算法求解的。

概括目前已知的求解ECDLP的算法,可以将它们分为2大类,即针对一般椭圆曲线的算法和针对特殊椭圆曲线的算法。本研究有价值之处在于通过详细分析目前已知的各种求解ECDLP的算法,提出1套完整的椭圆曲线的安全性准则。

1 一般椭圆曲线上ECDLP的求解算法

一般椭圆曲线上ECDLP的求解算法不依赖于

收稿日期:2003-09-30
基金项目:国家863计划基金资助课题(2001AA141010)
作者简介:文铁华(1965-),男,湖南醴陵人,博士

椭圆曲线的参数选取,普遍适应于各种椭圆曲线上的 ECDLP。下面一一介绍和分析其中效率较高的算法,并指出如何选择椭圆曲线以抵抗这些算法的攻击。

问题　已知 $|E(F_q)| = N$,P 为 $E(F_q)$ 的生成元,$Q \in E(F_q)$,求 l,使得 l 满足 $Q = lP(0 \le l \le N-1)$。

算法 1　Baby-Step Giant-Step (BSGS) 算法[3]

Step 1　(Giant-Step)　设 $M = [\sqrt{N}]$,计算并存储以下点序列 $OP, MP, 2MP, \cdots, (M-1)MP$ 于数据库中;

Step 2　(Baby-Step)　设函数 $f: E(F_q) \to E(F_q)$,$f(X) = X + P$,计算 $f^i(Q)$,$i = 0,1,\cdots$ 直至 $f^i(Q)$ 出现在数据库中,设 $f^i(Q) = Q + iP = (l+i)P = jMP$,则有 $l \equiv jM - i \bmod N$,问题解决。

该算法需要存储约 $\sqrt{N}$ 个点,算法的空间复杂度为 $O(\sqrt{N})$,在最坏情况下,Baby-Step 需要运算 $\sqrt{N}$ 步,算法的时间复杂度为 $O(\sqrt{N})$,是指数级的。当 N 足够大时,该算法失效。

算法 2　Pohlig-Hellman 算法[4]

Step 1　分解 $N = \prod_{i=0}^{t-1} p_i^{e_i}$(其中 P_i 均为素数,$i = 0,1,\cdots,t-1$);

Step 2　i 从 0 到 $t-l$ 重复下述步骤

1) 设 $l \equiv s_0 + s_1 p_i + \cdots + s_{e_i-1} p_i^{e_i-1} (\bmod\ p_i^{e_i})$,$0 \le s_j \le p_i - 1, j = 0,1,\cdots,e_{i-1}$;

2) 设 $P = (N/p_i)P$,$\overline{Q} = (N/p_i)Q$,则 $\overline{P}$ 和 $\overline{Q}$ 的阶均为 p_i,所以有以下等式成立:

$$\overline{Q} = (N/p_i)Q = (N/p_i)lp = l(N/p_i)P = l\overline{P} = s_0\overline{P}$$

求解该 ECDLP 问题,唯一确定 s_0。

3) 设 $\overline{P} = (N/pi)P$,$\overline{Q} = (N/p_i^2)(Q - s_0P)$,则有以下等式成立:

$$\overline{Q} = (N/p_i^2)(Q - s_0P) = (N/p_i^2)(l - s_0)P = s_1\overline{P}$$

求解该 ECDLP 问题,唯一确定 s_1,类似重复该过程直至完全唯一确定序列 $s_0, s_1, s_2, \cdots s_{e_i-1}$。

4) 根据系列 $s_0, s_1, s_2, \cdots s_{e_i-1}$ 可求出 $l_i \equiv l \bmod p_i^{e_i}$

Step 3　根据序列 $l_0, l_1, \cdots, l_{t-1}$,用中国剩余定理(CRT) 求解 l。

给定如下所述的 N,该算法将 ECDLP 分解成 $e_0 + e_1 + \cdots + e_{t-1} \le \lg N$ 个子 ECDLP。如果 N 的素因子 p_i 都很小($i = 0,1,\cdots,t-1$),则这些子 ECDLP都能用 BSGS算法求解。因此,为保证椭圆曲线的安全性,要求 N 有大的素因子,或者 N 本身就是素数,这样就可以保证用该算法求 ECDLP 时,其时间复杂度是指数级的。

算法 3　Pollard's Rho 算法[5]

Step 1　为了计算 l,首先将 $E(F_q)$ 划分为大致相等的 3 个集合:S_1、S_2 和 S_3;

Step 2　定义一个序列 r_i,$r_0 = P$,对于 $i \ge 0$,计算

$$r_{i+1} = \begin{cases} r_i + Q, \text{如果 } r_i \in S_1 \\ 2r_i, \text{如果 } r_i \in S_2 \\ r_i + P, \text{如果 } r_i \in S_3 \end{cases}$$

这样序列中的每个元素都形如 $r_i = a_iQ + b_iP$;

Step 3　计算上述序列,直至找到一个 i 使得 $r_i = r_{2i}$,即 $a_iQ + b_iP = a_{2i}Q + b_{2i}P$,令 $u = a_i - a_{2i}$,$v = b_{2i} - b_i$,从而得到

$$uQ = vP \tag{2}$$

Step 4　利用扩展欧几里得算法计算 $d = gcd(u, N) = \lambda u + \mu N$,从而得到 $\lambda u = d(\bmod N)$,代入式(2),得到 $dQ = \lambda vP$,必存在 $-k$,满足 $\lambda v \equiv dk(\bmod N)$,进而得到

$$q = kP + j(\frac{N}{d})P, \text{其中 } 0 \le j \le d-1$$

代入每个 j 的可能值,直到该等式成立,即求出 l。

Pollard's Rho 算法是时间复杂度为 $O(\sqrt{\pi n/2})$ 的概率算法。Oorschot 和 Wiener 将 Pollard's Rho 算法并行化[6],使得该算法在 r 个处理器并行执行时,时间复杂度下降为 $O((\sqrt{\pi n})/2r)$。Pollard's Rho 算法是目前已知的求解一般 ECDLP 的最有效的算法,但它仍然是指数级时间的复杂度。

Pollard 还提出的另一种概率算法,称为 Lambda 算法[5],与 Pollard's Rho 算法类似,Lambda 算法也可以并行化,但并行 Pollard's Lambda 算法稍慢于并行 Pollard's Rho 算法。但当搜索范围落在 $[0, N-1]$ 的子空间 $[0, b]$ 且 $b < 0.39N$ 时,Pollard's Lambda 算法的效率将高于 Pollard's Rho 算法。

需要指出的,在一般数域上的离散对数问题存在亚指数级时间复杂度的概率求解算法,即 Index Calculus 算法[7],但它不适应 ECDLP。Miller 以及 J. Silverman 和 Suzuki 都指出了 Index Calculus 算法对 ECDLP 问题不适用的原因[8]:无法在椭圆曲线上定义"smoothness" 集合。

是否存在一种求解 ECDLP 问题的亚指数级时间复杂度算法是一个一直没有解决的重要问题,关

系到ECC的安全性。想要证明求解ECDLP问题不存在一个亚指数级时间复杂度算法是很困难的。然而,通过过去对离散对数问题长达24 a的研究和对ECDLP问题长达16 a的研究表明,目前还没有发现求解ECDLP问题的亚指数级时间复杂度算法。

2 特殊椭圆曲线上ECDLP的求解算法

一些椭圆曲线,由于其某些参数选取的特殊性,使得其上的ECDLP存在有效的求解算法,即存在亚指数级时间复杂度甚至多项式时间复杂度的求解算法,因此这些特殊的椭圆曲线不能用来实现ECC。下面介绍特殊椭圆曲线上ECDLP的有效求解算法。

Menezes Okamoto 和 Vanstone[9] 以及 Frey 和 Rück[10] 的研究表明:定义在有限域 F_q 上的椭圆曲线 E 上的ECDLP问题可以约化为某些扩域 F_{q^k} 上的乘法群上的离散对数问题,从而可以使用NFS(Number Field Seive)算法进行求解。

算法4 MOV(Menezes Okamoto Vanstone)算法

Step 1 确定最小的正整数 k,使得 $E(F_q) \subseteq F_{q^k}$;

Step 2 选择 $R \in E(F_q)$,使得 $a = e_n(P,R)$ 的阶为 N,$e_n(P,R)$ 为Weil对(Weil Paring);

Step 3 计算 $\beta = e_n(Q,R)$;

Step 4 则在 F_{q^k} 上有 $\beta = a^l$ 成立,求解该离散对数问题,得出 l。

MOV约化算法仅当 k 很小的时候有效,而Balasubramanian和Koblitz的研究[11]表明:大部分椭圆曲线不满足这个条件。为了确保MOV约化算法不能应用到特定的椭圆曲线上,只需要确认基点 P 的阶 N 不能整除 $q^k - 1$,其中的 k 小至 F_{q^k} 上离散对数问题可以求解。目前,当 $N > 2^{192}$ 时,只需要确认基点 P 的阶 N 不能整除 $q^k - 1$,且 $1 \leq k \leq 20$,就足以抵抗MOV算法的攻击。

设 $|E(F_q)| = N$,则满足 $N = q + 1 - t$,其中 t 称为Frobenius映射的迹。迹 t 为0的椭圆曲线称为超奇异(Supersingular)椭圆曲线。可以证明这种椭圆曲线所对应的约化域的 $k \leq 6$,从而使得约化后的超奇异椭圆曲线上的ECDLP的MOV破解算法的时间复杂度降为亚指数级。因此,ECC实现不使用超奇异椭圆曲线,故在所有有关ECC的标准中都明确指出不采用超奇异椭圆曲线。可分解性检测排除了所有可以转化为 F_q 的小扩域的椭圆曲线,包括超奇异椭圆曲线和迹 $t = 2$(即 $|E(F_q)| = q - 1$)的椭圆曲线。

同MOV算法类似,FR(Frey Rück)算法可以亚指数级时间复杂度求解超奇异椭圆曲线上的ECDLP,这里不再祥述该算法。

SSSA(Semaev - Smart - Satoh - Araki)算法[2-4]是1个对反常(Anomalous)椭圆曲线上的ECDLP有效算法。反常椭圆曲线指的是迹 t 为1的椭圆曲线。Semaev,Smart以及Satoh和Araki研究给出了快速求解此类椭圆曲线上ECDLP的算法:该算法构造群同态,将 $E(F_q)$ 映射到 F_q^+,从而将 $E(F_q)$ 上的ECDLP转化为 F_q^+ 上的离散对数问题,而 F_q^+ 上的离散对数问题可以用欧几里德算法以多项式时间复杂度求解。因此,ECC实现不采用反常椭圆曲线。

还有一类特殊的椭圆曲线是奇异(Singular)椭圆曲线(曲线包含1个奇点),很容易通过构造群同态将奇异椭圆曲线上的ECDLP转化为 F_q^+ 上的离散对数问题(用欧几里德算法求解)或者 F_q^* 或 $F_{q^2}^*$ 上的离散对数问题(用NFS算法求解),因此奇异椭圆曲线也是不安全的。

超椭圆曲线(Hyperelliptic curve)是任意亏格(Genus)的一族代数曲线,包括椭圆曲线(Genus = 1)。对超椭圆曲线上的ECDLP,Adleman,DeMarrias和Huang提出了一种亚指数级时间复杂度的求解算法[15],最近出现的GHS算法[16],也可以有效地求解定义于二元扩域 F_{2^n} 的超椭圆曲线上的ECDLP。该类算法对求解有限域上的亏格较大的超椭圆曲线上ECDLP是亚指数级时间复杂度的,而对于椭圆曲线上ECDLP,则比穷举法的效果更差。

3 椭圆曲线的安全准则

通过对上述ECDLP求解算法的分析,我们知道:ECC的数学安全性依赖于所选椭圆曲线的安全性,特殊的椭圆曲线是有安全隐患的。为了抗击各种ECDLP攻击算法,我们给出下列ECC实现所选椭圆曲线的安全准则:

1) $E(F_q)$ 不是奇异椭圆曲线($t \neq 0$);

2) $E(F_q)$ 不是超奇异椭圆曲线($t \neq 1$);

3) $E(F_q)$ 不是反常椭圆曲线($t \neq 1$);

4) $|E(F_q)|$ 不等于 $q - 1$($t \neq 2$);

5) $|E(F_q)|$ 包含有大的素因子;

6) $|E(F_q)|$ 不能整除 $q^k - 1$,这里的 $1 \leq k \leq 20$;

7) 选择 $G \in E(F_q)$,且 G 的阶为 $|E(F_q)|$ 的

最大素因子,在 $E(F_q)$ 的子群(G)上实现 ECC。

根据上文的分析,我们知道:解决满足上述安全准则的椭圆曲线上的 ECDLP 的时间复杂度是指数级的。

4 结束语

介绍和分析了各种 ECDLP 的求解算法,指出抵抗这些算法攻击的椭圆曲线安全性要求,并最终得出一套完整的椭圆曲线安全性准则。说明了什么样的椭圆曲线是安全的这个问题,但并没有说明如何随机挑选安全的椭圆曲线的问题。要随机挑选安全的椭圆曲线,首先必须能计算椭圆曲线的阶($|E(F_q)|$),这是一项复杂的工作,目前解决这一问题的有效算法是 SEA 算法[17]。作者所在的研究小组改进了SEA算法并已形成软件工具,成功地解决了 $|E(F_q)|$ 的计算问题。

参考文献:

[1] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987(48):203 - 209.

[2] Miller V. Uses of elliptic curves in cryptography [A]. Advances in Cryptology - Crypto '85, LNCS 218 [C]. 1986.417 - 426.

[3] Shanks D. Class number, a theory of factorizations and genera [A]. Proceedings of Symposia in Pure Mathematics [C]. 1971. 415 - 440.

[4] Polig S C, Hellman M E. An improved algorithm over GF(p) and its cryptographic significance [J]. IEEE Transaction on Information Theory, 1978(24):106 - 110.

[5] Pollard J M. Monte Carlo methods for index computation (mod p)[J]. Mathematics of Computation, 1978(32):918 - 924.

[6] van Oorschot P C, Wiener M. Parallel collision search with cryptanalytic applications[J]. Journal of Cryptology, 1999,12 (12):1 - 28.

[7] McCurley K. The discrete logarithm problem [J]. Cryptology and Computational Number Theory, 1990,42:49 - 74.

[8] Silverman J H, Suzuki J. Elliptic curve discrete logarithms and the index calculus [A]. Proc of Asiacrypt '98[C]. 1998.110 - 125.

[9] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field [J]. IEEE Transaction on Information Theory, 1993(5):1 639 - 1 646.

[10] Frey G, Ruck H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves [J]. Mathematics of Computation, 1994,62:865 - 874.

[11] Balasubramanian R, Koblitz N. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes - Okamoto - Vanstone algorithm [J]. Journal of Cryptology, 1998, 11:141 - 145.

[12] Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves [J]. Commentarii Mathematici Universitatis Sancti Pauli, 1998, 47:81 - 92.

[13] Semaev I. Evaluation of discrete logarithms in a group of p - torsion points of an elliptic curve in characteristic [J]. Mathematics of Computation, 1998, 67(221):353 - 356.

[14] Smart N P. The discrete logarithms problem on elliptic curves of trace one [J]. Journal of Cryptology, 1999,12: 193 - 196.

[15] Adleman L, Demarrais J, Huang M D. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobian of large genus hyperelliptic curves over finite fields [A]. Proc First Int'l Symp on Algorithmic Number Theory (ANTS - 1)[C]. 1994.28 - 40.

[16] Gaudry P, Hess F, Smart N. Constructive and destructive facets of Weil descent on elliptic curves [J]. Journal of Cryptology, 2002,15:19 - 46.

[17] Schoof R. Counting points on elliptic curves over finite fields [J]. Journal Theorie des Nombres de Bordeaux, 1995,7: 219 - 254.